

Interference Search

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	7	CONTENT AND "DIGITAL CERTIFICATE" AND "REMOTE SERVER" AND CLIENT AND ENCRYPT\$3 AND KEY\$1 AND DRM	US-PGPUB; USPAT	OR	OFF	2005/11/14 20:19
L2	7	CONTENT AND "DIGITAL CERTIFICATE" AND "REMOTE SERVER" AND CLIENT AND ENCRYPT\$3 AND KEY\$1 AND DRM	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/11/14 20:18
L3	0	CONTENT.CLM. AND "DIGITAL CERTIFICATE".CLM. AND "REMOTE SERVER".CLM. AND CLIENT.CLM. AND ENCRYPT\$3. CLM. AND KEY\$1.CLM. AND DRM. CLM.	US-PGPUB	OR	OFF	2005/11/14 20:20
L4	X 0	CONTENT.CLM. AND "DIGITAL CERTIFICATE".CLM. AND "REMOTE SERVER".CLM. AND CLIENT.CLM. AND ENCRYPT\$3. CLM. AND KEY\$1.CLM. AND DRM. CLM.	US-PGPUB; USPAT	OR	OFF	2005/11/14 20:20
L5	X 0	CONTENT.CLM. AND "DIGITAL CERTIFICATE".CLM. AND "REMOTE SERVER".CLM. AND CLIENT.CLM. AND ENCRYPT\$3. CLM. AND KEY\$1.CLM.	US-PGPUB; USPAT	OR	OFF	2005/11/14 20:20
L6	X 8	CONTENT.CLM. AND "DIGITAL CERTIFICATE".CLM. AND SERVER. CLM. AND CLIENT.CLM. AND ENCRYPT\$3.CLM. AND KEY\$1. CLM.	US-PGPUB; USPAT	OR	OFF	2005/11/14 20:20

updated Search

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	7	CONTENT AND "DIGITAL CERTIFICATE" AND "REMOTE SERVER" AND CLIENT AND ENCRYPT\$3 AND KEY\$1 AND DRM	US-PGPUB; USPAT	OR	OFF	2005/11/14 20:19
L2	7	CONTENT AND "DIGITAL CERTIFICATE" AND "REMOTE SERVER" AND CLIENT AND ENCRYPT\$3 AND KEY\$1 AND DRM	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/11/14 20:18
L3	0	CONTENT.CLM. AND "DIGITAL CERTIFICATE".CLM. AND "REMOTE SERVER".CLM. AND CLIENT.CLM. AND ENCRYPT\$3. CLM. AND KEY\$1.CLM. AND DRM. CLM.	US-PGPUB	OR	OFF	2005/11/14 20:20
L4	0	CONTENT.CLM. AND "DIGITAL CERTIFICATE".CLM. AND "REMOTE SERVER".CLM. AND CLIENT.CLM. AND ENCRYPT\$3. CLM. AND KEY\$1.CLM. AND DRM. CLM.	US-PGPUB; USPAT	OR	OFF	2005/11/14 20:20
L5	0	CONTENT.CLM. AND "DIGITAL CERTIFICATE".CLM. AND "REMOTE SERVER".CLM. AND CLIENT.CLM. AND ENCRYPT\$3. CLM. AND KEY\$1.CLM.	US-PGPUB; USPAT	OR	OFF	2005/11/14 20:20
L6	8	CONTENT.CLM. AND "DIGITAL CERTIFICATE".CLM. AND SERVER. CLM. AND CLIENT.CLM. AND ENCRYPT\$3.CLM. AND KEY\$1. CLM.	US-PGPUB; USPAT	OR	OFF	2005/11/14 20:20
L7	777	713/156	US-PGPUB; USPAT	OR	OFF	2005/11/14 20:21
L8	2440	713/156 OR 713/167 OR 713/175 OR 713/193	US-PGPUB; USPAT	OR	OFF	2005/11/14 20:21
L9	3	8 AND 1	US-PGPUB; USPAT	OR	OFF	2005/11/14 20:21

[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)

PORTAL [USPTO](#)

Search: The ACM Digital Library The Guide

"digital certificate" and profile and server and encrypt\$3 and key\$1 and hardware and remote

THE ACM DIGITAL LIBRARY

 [Feedback](#) [Report a problem](#) [Satisfaction survey](#)

Terms used [digital certificate](#) and [profile](#) and [server](#) and [encrypt\\$3](#) and [key\\$1](#) and [hardware](#) and [remote](#) Found 9,591 of 166,357

Sort results by [relevance](#) Save results to a Binder [Try an Advanced Search](#)
 Display results [expanded form](#) Open results in a new window [Try this search in The ACM Guide](#)

Results 1 - 20 of 200 Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

Best 200 shown

Relevance scale 

1 Ad hoc network: A security design for a general purpose, self-organizing, multihop ad hoc wireless network 

Thomas S. Messerges, Johnas Cukier, Tom A. M. Kevenaar, Larry Puhl, René Struik, Ed Callaway
 October 2003 **Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks**

Publisher: ACM Press

Full text available:  [pdf\(353.25 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

We present a security design for a general purpose, self-organizing, multihop ad hoc wireless network, based on the IEEE 802.15.4 low-rate wireless personal area network standard. The design employs elliptic-curve cryptography and the AES block cipher to supply message integrity and encryption services, key-establishment protocols, and a large set of extended security services, while at the same time meeting the low implementation cost, low power, and high flexibility requirements of ad hoc wire ...

Keywords: 802.15.4, ad hoc networks, security, wireless

2 Security in embedded systems: Design challenges 
 Srivaths Ravi, Anand Raghunathan, Paul Kocher, Sunil Hattangady
 August 2004 **ACM Transactions on Embedded Computing Systems (TECS)**, Volume 3 Issue 3

Publisher: ACM Press

Full text available:  [pdf\(3.67 MB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#), [review](#)

Many modern electronic systems---including personal computers, PDAs, cell phones, network routers, smart cards, and networked sensors to name a few---need to access, store, manipulate, or communicate sensitive information, making security a serious concern in their design. Embedded systems, which account for a wide range of products from the electronics, semiconductor, telecommunications, and networking industries, face some of the most demanding security concerns---on the one hand, they are oft ...

Keywords: Embedded systems, architecture, authentication, battery life, cryptographic algorithms, decryption, encryption, hardware design, processing requirements, security, security attacks, security protocols, tamper resistance

3 Design and modelling of internode: a mobile provider provisioned VPN

Francisco Barceló, Josep Paradells, Fofy Setaki, Monique Gibeaux
February 2003 **Mobile Networks and Applications**, Volume 8 Issue 1

Publisher: Kluwer Academic Publishers

Full text available:  pdf(237.48 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

This paper presents the design and architecture of a mobile Provider Provisioned VPN (PPVPN) together with a performance evaluation oriented model that allows first estimates of the VPN set-up delay to be computed. At the same time, some consequences of the discussion can be applied to the design of the VPN configuration parameters. Many different technologies and protocols are used: access is supplied through GPRS or WaveLANs, IP mobility is supported by Mobile IP, and the VPN is based on the I ...

Keywords: IPSec, VPN, mobile IP, mobile VPN, provider provisioned VPN

4 Proxy-based acceleration of dynamically generated content on the world wide web:

 **An approach and implementation**

Anindya Datta, Kaushik Dutta, Helen Thomas, Debra Vandermeer, Krithi Ramamritham
June 2004 **ACM Transactions on Database Systems (TODS)**, Volume 29 Issue 2

Publisher: ACM Press

Full text available:  pdf(927.23 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

As Internet traffic continues to grow and websites become increasingly complex, performance and scalability are major issues for websites. Websites are increasingly relying on dynamic content generation applications to provide website visitors with dynamic, interactive, and personalized experiences. However, dynamic content generation comes at a cost---each request requires computation as well as communication across multiple components. To address these issues, various dynamic content caching ap ...

Keywords: Edge caching, caching dynamically generated content, fragment caching, implementation, proxy caching, world wide web

5 Gauging the risks of internet elections

 Deborah M. Phillips, Hans A. von Spakovsky

January 2001 **Communications of the ACM**, Volume 44 Issue 1

Publisher: ACM Press

Full text available:  pdf(159.11 KB)  html(35.52 KB) Additional Information: [full citation](#), [references](#), [index terms](#)

6 The case for internet voting

 Joe Mohen, Julia Glidden

January 2001 **Communications of the ACM**, Volume 44 Issue 1

Publisher: ACM Press

Full text available:  pdf(158.11 KB)  html(35.34 KB) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

7 Index structures for selective dissemination of information under the Boolean model

Tak W. Yan, Héctor García-Molina
June 1994

ACM Transactions on Database Systems (TODS), Volume 19 Issue 2

Publisher: ACM Press

Full text available:  pdf(2.03 MB)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#), [review](#)

The number, size, and user population of bibliographic and full-text document databases are rapidly growing. With a high document arrival rate, it becomes essential for users of such databases to have access to the very latest documents; yet the high document arrival rate also makes it difficult for users to keep themselves updated. It is desirable to allow users to submit profiles, i.e., queries that are constantly evaluated, so that they will be automatically informed of new additions tha ...

8 A secure infrastructure for service discovery and access in pervasive computing 

Jeffrey Undercoffer, Filip Perich, Andrej Cedilnik, Lalana Kagal, Anupam Joshi

April 2003 **Mobile Networks and Applications**, Volume 8 Issue 2

Publisher: Kluwer Academic Publishers

Full text available:  pdf(308.34 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

Security is paramount to the success of pervasive computing environments. The system presented in this paper provides a communications and security infrastructure that goes far in advancing the goal of anywhere-anytime computing. Our work securely enables clients to access and utilize services in heterogeneous networks. We provide a service registration and discovery mechanism implemented through a hierarchy of service management. The system is built upon a simplified Public Key Infrastructure t ...

Keywords: distributed services, extensible markup language, pervasive computing, security, smartcards

9 XML security: Certificate validation service using XKMS for computational grid 

Namje Park, Kiyoung Moon, Sungwon Sohn

October 2003 **Proceedings of the 2003 ACM workshop on XML security**

Publisher: ACM Press

Full text available:  pdf(7.01 MB)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

A computational grid is a hardware and software infrastructure capable of providing dependable, consistent, pervasive, and inexpensive access to high-end computational resource. There are many ways to access the resources of a computational grid, each with unique security requirements and implications for both the resource user and the resource provider. Current Grid security Infrastructure using PKI based on SSO. But open grid service Security Infrastructure in Global Grid Forum(GGF) will exten ...

Keywords: GSI, XKMS, XML, XML security, certificate validation, grid, key management, security

10 Security as a new dimension in embedded system design: Security as a new dimension in embedded system design 

Srivaths Ravi, Paul Kocher, Ruby Lee, Gary McGraw, Anand Raghunathan

June 2004 **Proceedings of the 41st annual conference on Design automation**

Publisher: ACM Press

Full text available:  pdf(209.10 KB)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

The growing number of instances of breaches in information security in the last few years has created a compelling case for efforts towards secure electronic systems. Embedded

systems, which will be ubiquitously used to capture, store, manipulate, and access data of a sensitive nature, pose several unique and interesting security challenges. Security has been the subject of intensive research in the areas of cryptography, computing, and networking. However, despite these efforts, *security is ...*

Keywords: PDAs, architectures, battery life, cryptography, design, design methodologies, digital rights management, embedded systems, performance, security, security processing, security protocols, sensors, software attacks, tamper resistance, trusted computing, viruses

11 SaveMe: a system for archiving electronic documents using messaging groupware

Stefan Berchtold, Alexandros Biliris, Euthimios Panagos

March 1999 **ACM SIGSOFT Software Engineering Notes , Proceedings of the international joint conference on Work activities coordination and collaboration WACC '99**, Volume 24 Issue 2

Publisher: ACM Press

Full text available:  pdf(1.47 MB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Today, organizations deal with an ever-increasing number of documents that have to be archived because they are either related to their core business (e.g., product designs) or needed to meet corporate or legal retention requirements (e.g., voucher). In this paper, we present the architecture and prototype implementation of SaveMe, a document archival system that is based on network-centric groupware such as Internet standards-based messaging systems. In SaveMe, the actions of archiving, retriev ...

Keywords: Internet, archiving, groupware, messaging

12 Columns: Risks to the public in computers and related systems

Peter G. Neumann

July 2001 **ACM SIGSOFT Software Engineering Notes**, Volume 26 Issue 4

Publisher: ACM Press

Full text available:  pdf(1.17 MB) Additional Information: [full citation](#)

13 The middleware muddle

David Ritter

December 1998 **ACM SIGMOD Record**, Volume 27 Issue 4

Publisher: ACM Press

Full text available:  pdf(543.46 KB) Additional Information: [full citation](#), [abstract](#), [index terms](#)

A new menagerie of middleware is emerging. These products promise great flexibility in partitioning enterprise applications across the diverse corporate computing landscape.

What factors should you consider when choosing a solution, and how do current products stack up? More important to the focus of this article, what role should Web servers play?

14 Applications: A context-related authorization and access control method based on

RBAC:

Marc Wilikens, Simone Feriti, Alberto Sanna, Marcelo Masera

June 2002 **Proceedings of the seventh ACM symposium on Access control models and technologies**

Publisher: ACM Press

Full text available:  pdf(260.70 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

This paper describes an application of authorization and access control based on the Role Based Access Control (RBAC) method and integrated in a comprehensive trust infrastructure of a health care application. The method is applied to a health care business process that involves multiple actors accessing data and resources needed for performing clinical and logistics tasks in the application. The notion of trust constituency is introduced as a concept for describing the context of authorisation. ...

Keywords: role based access control (RBAC), secure health care system, trust infrastructure

15 Session I - supporting face-to-face groups: A group decision support system for idea 

 **generation and issue analysis in organization planning**

Lynda M. Applegate, Benn R. Konsynski, J. F. Nunamaker

December 1986 **Proceedings of the 1986 ACM conference on Computer-supported cooperative work**

Publisher: ACM Press

Full text available:  pdf(1.38 MB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#)

The increasing reliance on group decision-making in today's complex business environments and advances in microcomputer, telecommunications and graphic presentation technology have combined to create a growing interest in the design of group decision support systems (GDSS). Planning is an important group decision-making activity within organizations. Effective planning depends on the generation and analysis of innovative ideas. For this reason, the idea generation and management process has been ...

16 Managing battery lifetime with energy-aware adaptation 

 Jason Flinn, M. Satyanarayanan

May 2004 **ACM Transactions on Computer Systems (TOCS)**, Volume 22 Issue 2

Publisher: ACM Press

Full text available:  pdf(1.61 MB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

We demonstrate that a collaborative relationship between the operating system and applications can be used to meet user-specified goals for battery duration. We first describe a novel profiling-based approach for accurately measuring application and system energy consumption. We then show how applications can dynamically modify their behavior to conserve energy. We extend the Linux operating system to yield battery lifetimes of user-specified duration. By monitoring energy supply and demand and ...

Keywords: Power management, adaptation

17 Using Hardware Counters to Automatically Improve Memory Performance 

Mustafa M. Tikir, Jeffrey K. Hollingsworth

November 2004 **Proceedings of the 2004 ACM/IEEE conference on Supercomputing**

Publisher: IEEE Computer Society

Full text available:  pdf(152.84 KB) Additional Information: [full citation](#), [abstract](#)

In this paper, we introduce a profile-driven online page migration scheme and investigate its impact on the performance of multithreaded applications. We use lightweight, inexpensive plug-in hardware counters to profile the memory access behavior of an application, and then migrate pages to memory local to the most frequently accessing processor. Using the Dyninst runtime instrumentation combined with hardware counters, we were able to add page migration capabilities to the system without having ...

18 MemorIES3: a programmable, real-time hardware emulation tool for multiprocessor server design

Ashwini Nanda, Kwok-Ken Mak, Krishnan Sugavanam, Ramendra K. Sahoo, Vijayaraghavan Soundararajan, T. Basil Smith

November 2000 **ACM SIGOPS Operating Systems Review , ACM SIGARCH Computer Architecture News , Proceedings of the ninth international conference on Architectural support for programming languages and operating systems ASPLOS-IX**, Volume 34 , 28 Issue 5 , 5

Publisher: ACM Press

Full text available: [pdf\(724.53 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

Modern system design often requires multiple levels of simulation for design validation and performance debugging. However, while machines have gotten faster, and simulators have become more detailed, simulation speeds have not tracked machine speeds. As a result, it is difficult to simulate realistic problem sizes and hardware configurations for a target machine. Instead, researchers have focussed on developing scaling methodologies and running smaller problem sizes and configurations that atte ...

19 MemorIES: a programmable, real-time hardware emulation tool for multiprocessor server design

Ashwini Nanda, Kwok-Ken Mak, Krishnan Sugavanam, Ramendra K. Sahoo, Vijayaraghavan Soundararajan, T. Basil Smith

November 2000 **ACM SIGPLAN Notices**, Volume 35 Issue 11

Publisher: ACM Press

Full text available: [pdf\(1.84 MB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Modern system design often requires multiple levels of simulation for design validation and performance debugging. However, while machines have gotten faster, and simulators have become more detailed, simulation speeds have not tracked machine speeds. As a result, it is difficult to simulate realistic problem sizes and hardware configurations for a target machine. Instead, researchers have focussed on developing scaling methodologies and running smaller problem sizes and configurations that atte ...

20 Multigrain shared memory

Donald Yeung, John Kubiatowicz, Anant Agarwal

May 2000 **ACM Transactions on Computer Systems (TOCS)**, Volume 18 Issue 2

Publisher: ACM Press

Full text available: [pdf\(369.18 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#), [review](#)

Parallel workstations, each comprising tens of processors based on shared memory, promise cost-effective scalable multiprocessing. This article explores the coupling of such small- to medium-scale shared-memory multiprocessors through software over a local area network to synthesize larger shared-memory systems. We call these systems Distributed Shared-memory MultiProcessors (DSMPs). This article introduces the design of a shared-memory system that uses multiple granularities of sharing, ca ...

Keywords: distributed memory, symmetric multiprocessors, system of systems